8.5 Network Management

Georgia Technology Authority

Network Controls

POLICY NUMBER: 8.5.1	EFFECTIVE DATE: April 1, 2005

PURPOSE

- To require controls for the security of data on networks
- To protect connected services from unauthorized access.

SCOPE

This policy addresses the requirement for controls to safeguard information on all State of Georgia information systems networks and to protect the supporting infrastructure of such networks.

POLICY

Agencies should establish controls to ensure the security of the information systems networks that they operate.

FIREWALL SECURITY STANDARDS for Agency Managed Firewalls

General: Firewalls must be placed such that agencies have firewalls at a minimum between them and the state backbone, and not rely solely on the state gateway firewalls for protection.

Firewall Business Owner: Agencies must designate a specific individual or position responsible for Firewall configurations (e.g. Agency ISO or Agency CIO/IT Director or their designee). Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to individuals authorized by the Agency ISO.

Default Denial: Agency firewalls must block every network connectivity path and network service not specifically authorized by the Agency ISO.

Firewall Physical Security: State agencies must employ due diligence in ensuring physical security at any location where firewalls will be installed.

Rule Documentation: All changes to firewall configuration parameters, enabled services, and permitted connectivity must be documented.

Firewall Logs: Use and maintenance of Firewall logging capability (where available) is at Agency’s discretion.

Record Retention: All documentation and/or firewall logs should be retained in accordance with each agency's respective retention policies and schedules. No specific retention requirements are set forth by these Standards.

Periodic Review: Firewall configuration must be reviewed to ensure compliance to agency or State security policies. Supporting documentation must exist for all enabled services. Agencies are responsible for testing their firewall configuration(s) for effectiveness.

Posting Updates: Agency personnel responsible for managing firewalls will subscribe to security advisories and other relevant sources providing up-to-date information about firewall vulnerabilities.

GUIDELINES

Because the guidelines around firewall rules are changing continuously, and for security reasons, firewall rule guidelines are available to state agencies by request to the GTA Policy Group (GTAPSG@gta.ga.gov)